COMMONWEALTH of VIRGINIA

Department of Information Technology

110 SOUTH SEVENTH STREET
RICHMOND, VIRGINIA 23219
(804) 371-5000

NETWORK SECURITY ADVISORY

To: MIS Directors
Security Officers

From: Don Kendrick,
Chief Security Architect

Re: W32/SQLSlammer.worm

Date: 27 January 2003

Over the weekend a new worm has appeared. This worm, currently called W32/SQLSlammer.worm, may have an impact on network traffic over the next few days and create "Denial of Service" conditions as it attempts to propagate.

This worm exploits a known vulnerability in Microsoft SQL Server 2000 Server Resolution service. SQL Server 2000 installations with Service Pack 2 and earlier are vulnerable. Service Pack 3 does correct the vulnerability as well as MS02-61 (which supercedes patch MS02-039).

Most AV programs will not detect this worm. However, if you do discover that you are infected, a simple reboot should clear the server since it appears that this worm only exists in memory.

All users of SQL Server 2000 are strongly urged to check their patch levels immediately and insure that they are protected.

This attack uses port 1434/UDP. Of course, security best practices would suggest that any site should not have their SQL servers exposed to the world and would be practicing a default deny stance to traffic.

In the event that this Worm begins to create "Denial of Service" conditions, it is suggested that organizations begin blocking this specific port as far out on their perimeter as they can (even

requesting ISP assistance if needed).

Don

****

Don Kendrick, CNE, CCNA, GCIA, CISSP
Chief Security Architect
Commonwealth of Virginia
Department of Information Technology
(804) 371-5715
110 S. 7th Street
Richmond, Virginia 23219

"Keep your arms and hands inside the car and enjoy your ride..."